

COMPUTER SECURITY

SYMMETRIC-KEY
CRYPTOGRAPHY
(BLOCK CIPHERS)

Willy Sudiarto Raharjo

Teknik Informatika
Universitas Kristen Duta Wacana

Block Ciphers

- Plaintext and ciphertext consist of fixed-sized blocks
- Ciphertext obtained from plaintext by iterating a **round function**
- Input to round function consists of *key* and *output* of previous round
- Usually implemented in software

Block Ciphers

- Replaces a block of N plaintext bits with a block of N ciphertext bits (N = block size) using iterated F function

$$\text{Ciphertext} = F(\text{plaintext})$$

- The exact transformation is controlled using a second input — the secret key
- Design goal
 - ◆ Security
 - ◆ Efficiency

Feistel Cipher

- Designed by Horst Feistel
- General cipher design principle (input: data block + key)
- Plaintext P is split into left and right halves

$$P = (L_0, R_0)$$

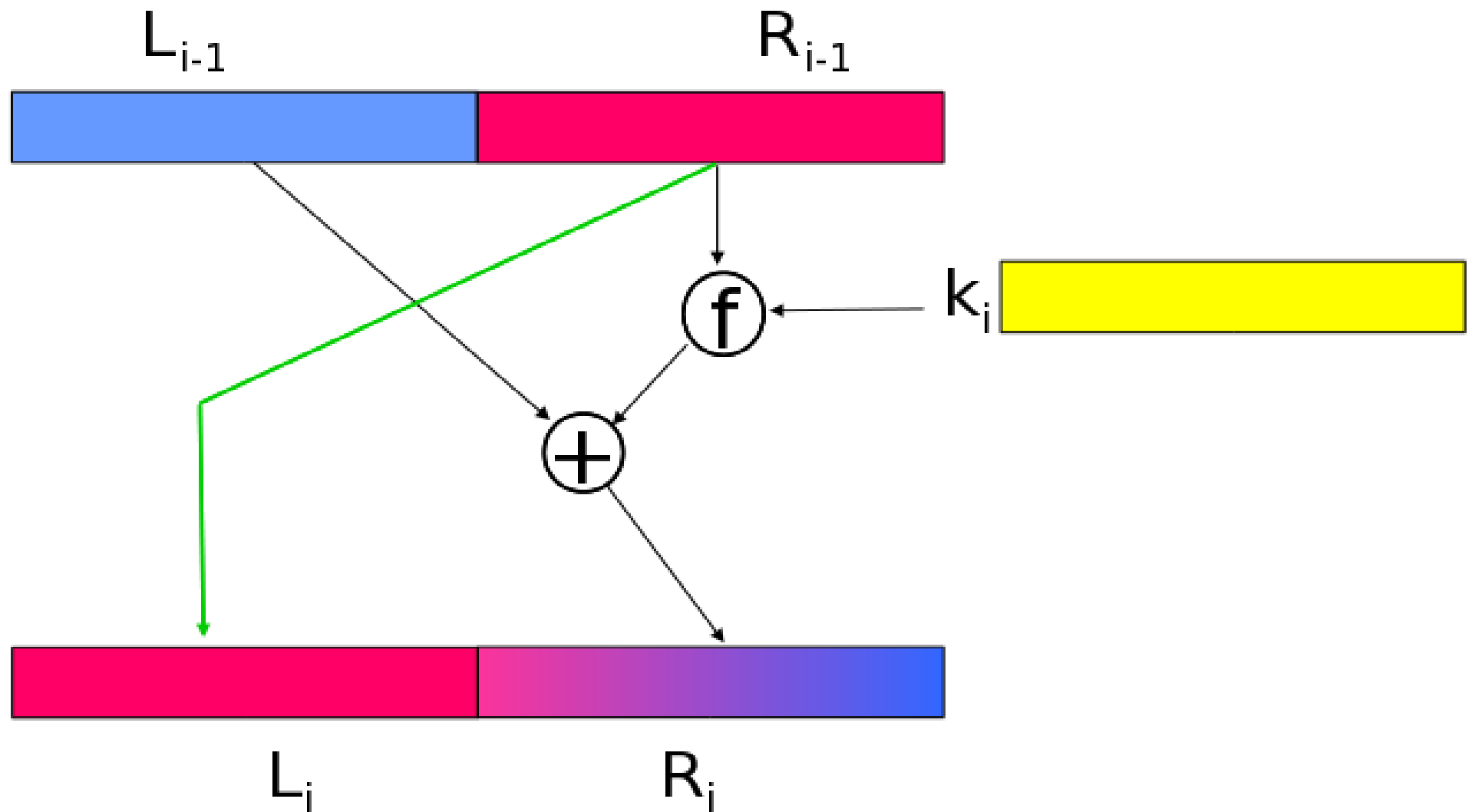
- For each round i new left and right halves are computed

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

- K_i is the subkey for round i . Subkey is derived from key K according to key schedule algorithm

Round i



Feistel Cipher

- Ciphertext C is the output of the final round

$$C = (L_n, R_n)$$

- Decryption works by reversing the order for R_{i-1} and L_{i-1}

$$R_{i-1} = L_i$$

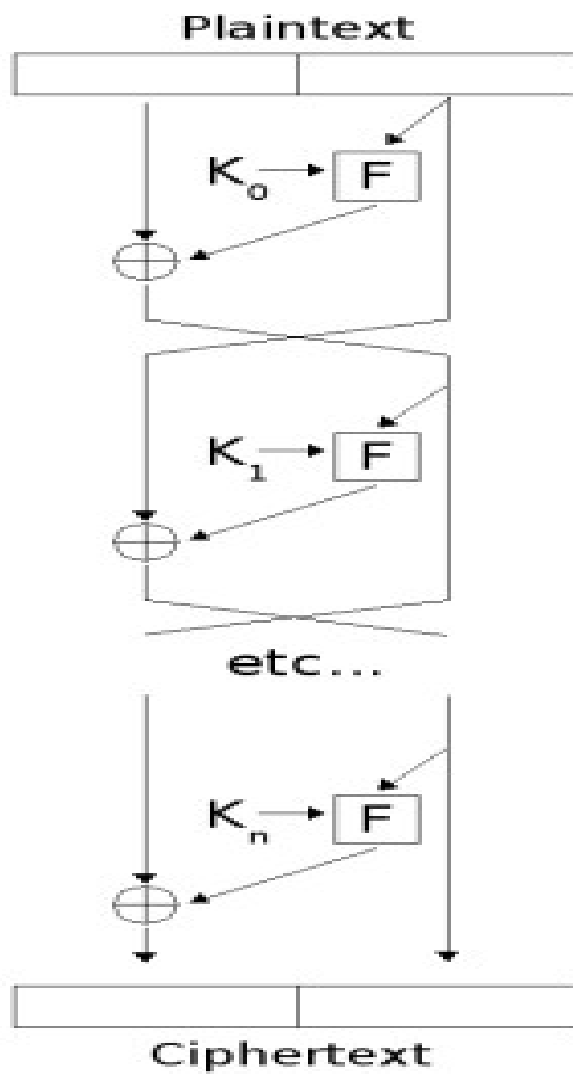
$$L_{i-1} = R_i \oplus F(R_{i-1}, K_i)$$

- The final result is the original plaintext

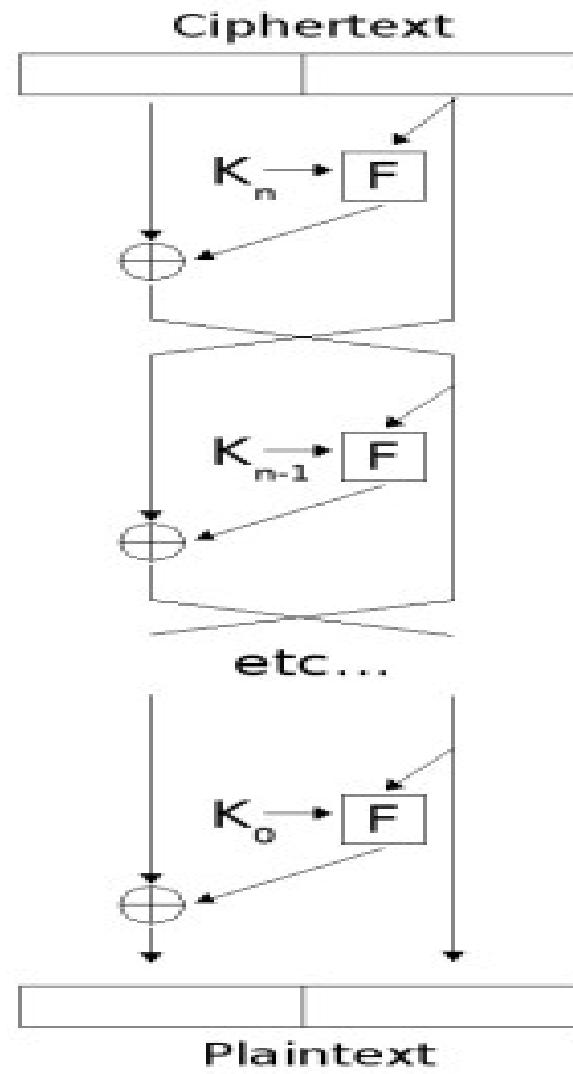
$$P = (L_0, R_0)$$

- Any round function F will work in Feistel cipher as long as the output of F produce correct number of bits

Encryption:



Decryption:

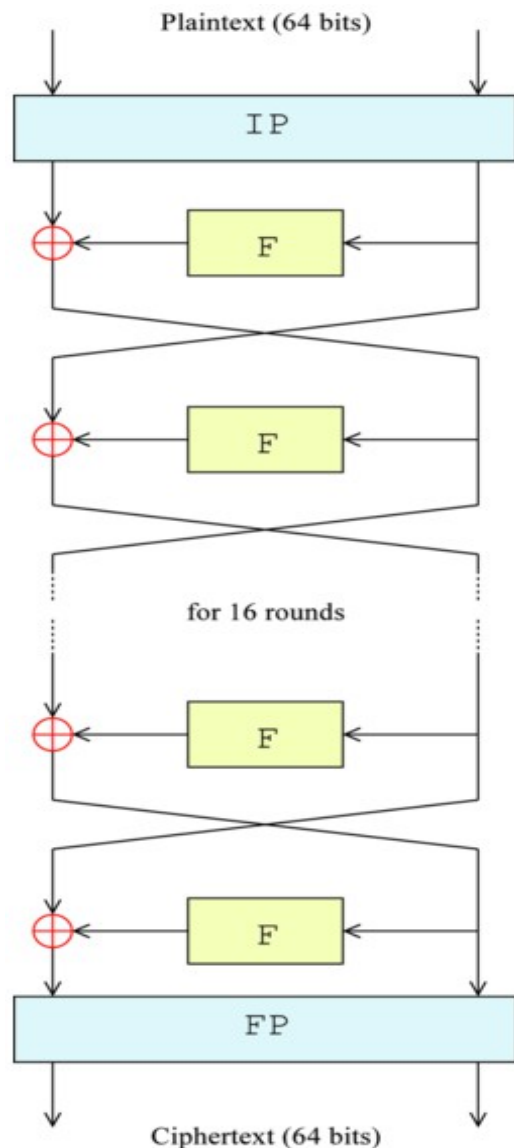


Feistel Cipher

DES: Data Encryption Standard

- Most widely used block cipher in the world
- Adopted by NIST in 1977
- Based on the Feistel cipher
 - 16 rounds of processing
 - Each round i uses a 48-bit subkey k_i
 - Block length = 64 bits
 - Key length = 56 bits (actual key = 64, 8 are discarded)
 - Keyspace: 2^{56} : 72.057.594.037.927.940
- At the very beginning, there is an initial permutation (IP)
- What is specific to DES is the design of the F function and how round keys are derived from the main key

DES Encryption Overview



- Block is divided into two 32-bit halves and processed using feistel structure
- The F-function scrambles half a block together with key
- The output from the F-function is then combined with the other half of the block, and the halves are swapped before the next round
- After the final round, the halves are not swapped
- Decryption works in reverse orders

Initial Permutation

(a) Initial Permutation (IP)

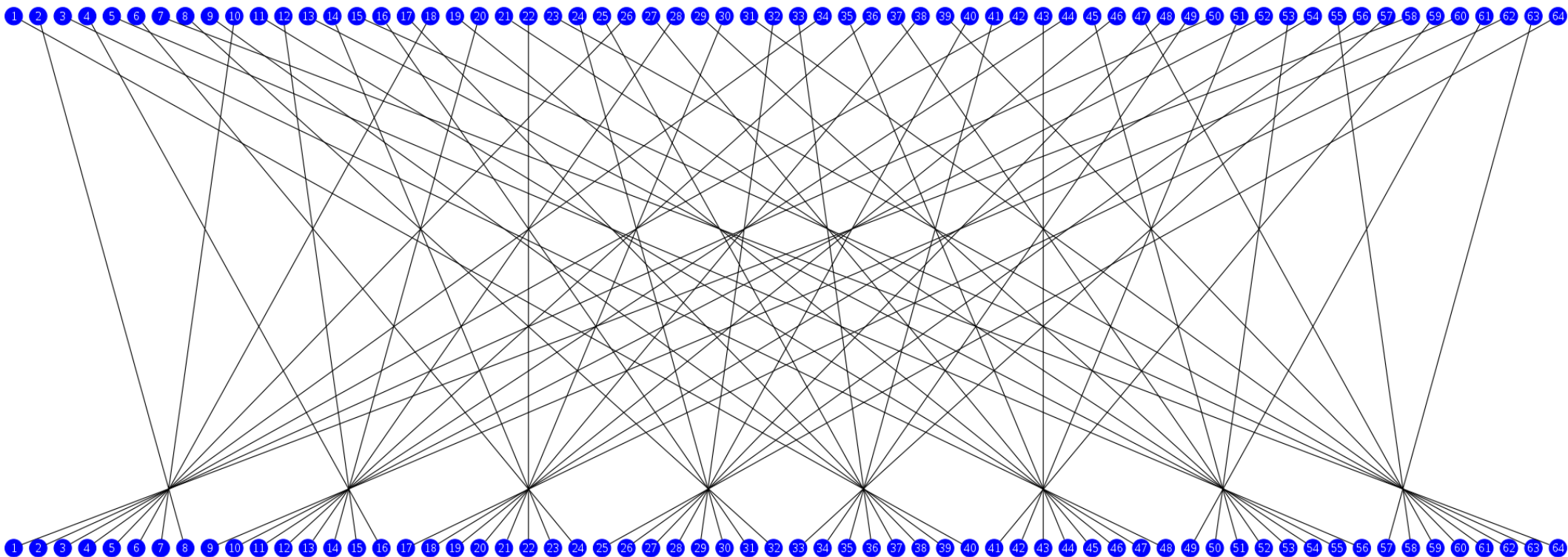
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

(b) Inverse Initial Permutation (IP^{-1})

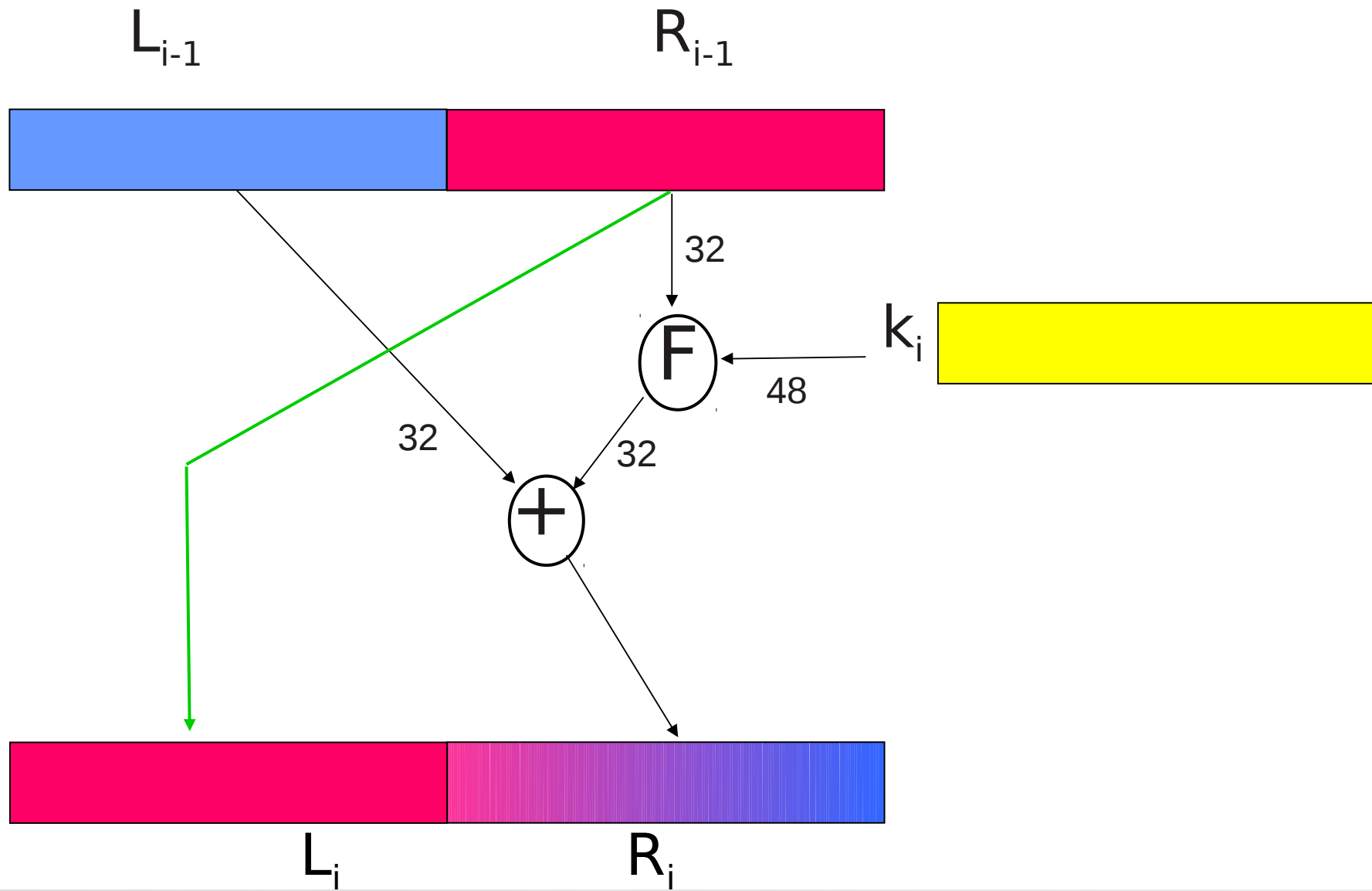
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

• bit	goes to bit	bit	goes to bit
• 58	1	57	33
• 50	2	49	34
• 42	3	41	35
• 34	4	33	36
• 26	5	25	37
• 18	6	17	38
• 10	7	9	39
• 2	8	1	40
• 60	9	59	41
• 52	10	51	42
• 44	11	43	43
• 36	12	35	44
• 28	13	27	45
• 20	14	19	46
• 12	15	11	47
• 4	16	3	48
• 62	17	61	49
• 54	18	53	50
• 46	19	45	51
• 38	20	37	52
• 30	21	29	53
• 22	22	21	54
• 14	23	13	55
• 6	24	5	56
• 64	25	63	57
• 56	26	55	58
• 48	27	47	59
• 40	28	39	60
• 32	29	31	61
• 24	30	23	62
• 16	31	15	63
• 8	32	7	64
•			

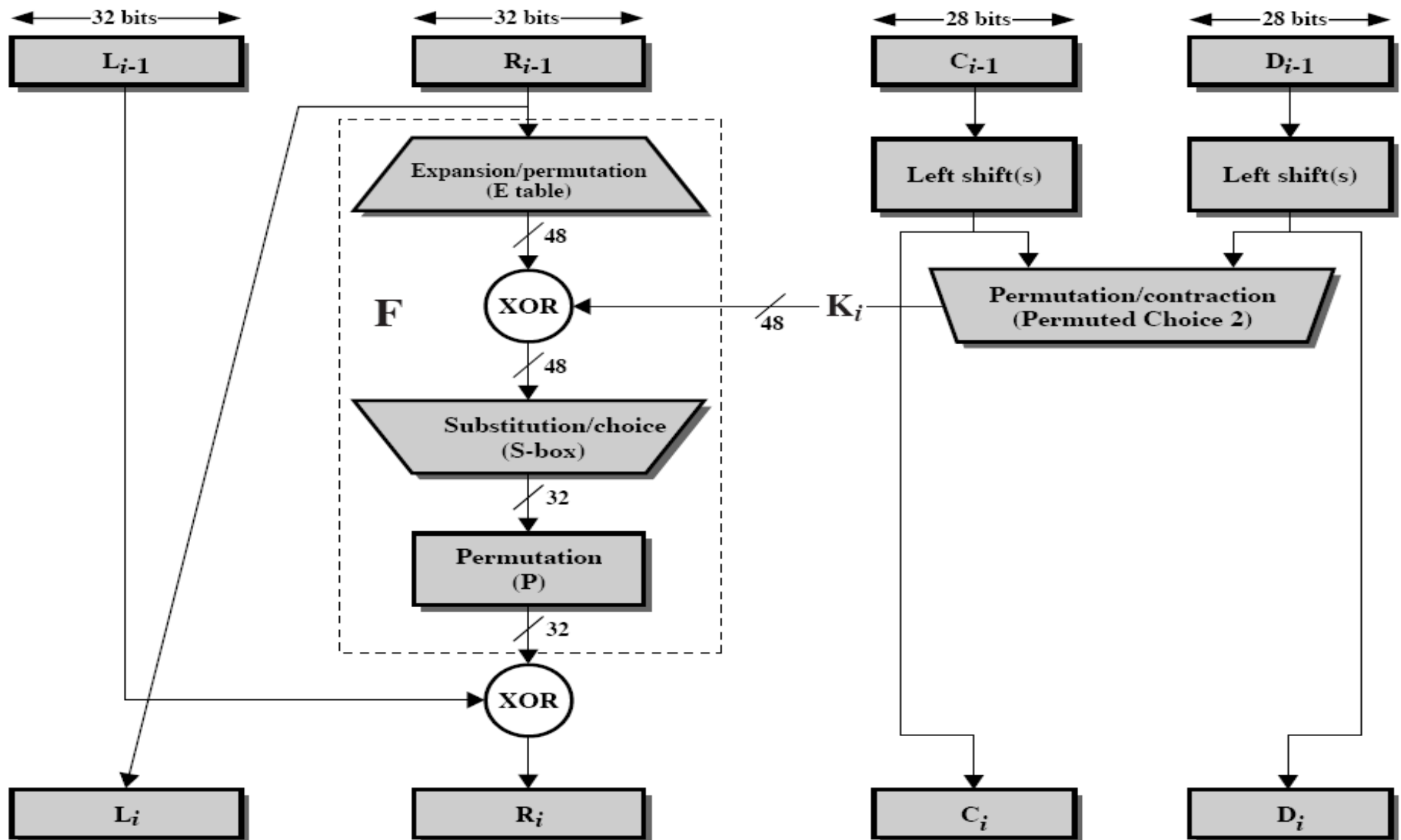
Initial Permutation Mapping



Round i



Single Round of DES



F Function

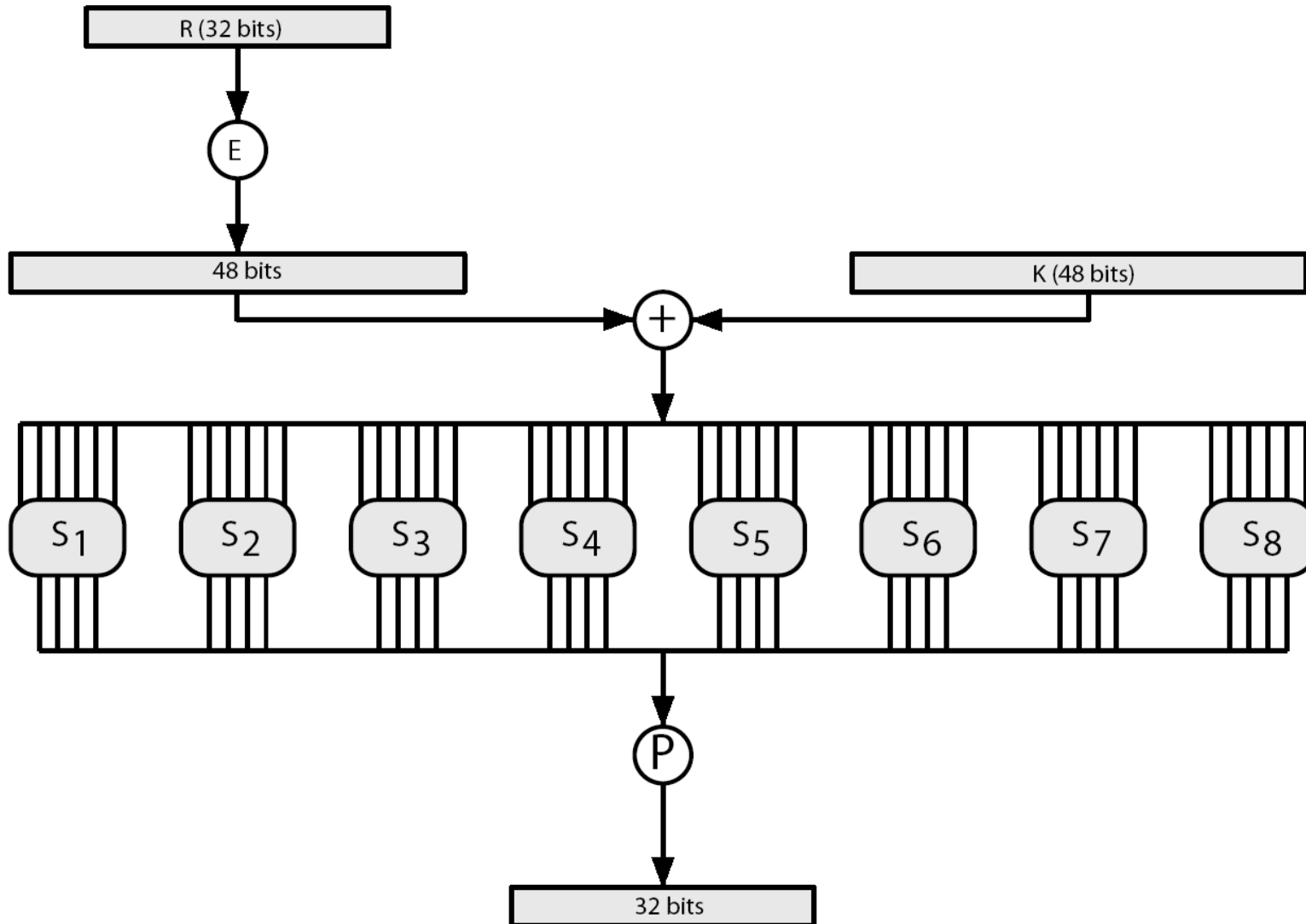
- Consists of

- **Expansion** permutation
 - Expand input from 32 to 48 bits (output)
 - Output (48 bits) is XORed with subkey (**Key Mixing**)
- **S-Boxes** (8 S-Boxes in DES)
 - Compress 48 bits → 32 bits before processed by P-Box (**Substitution**)
- **P-Box** (**P**ermutation Box, 2 in DES)
 - Output of P-Box is XORed with old left half to obtain new right half

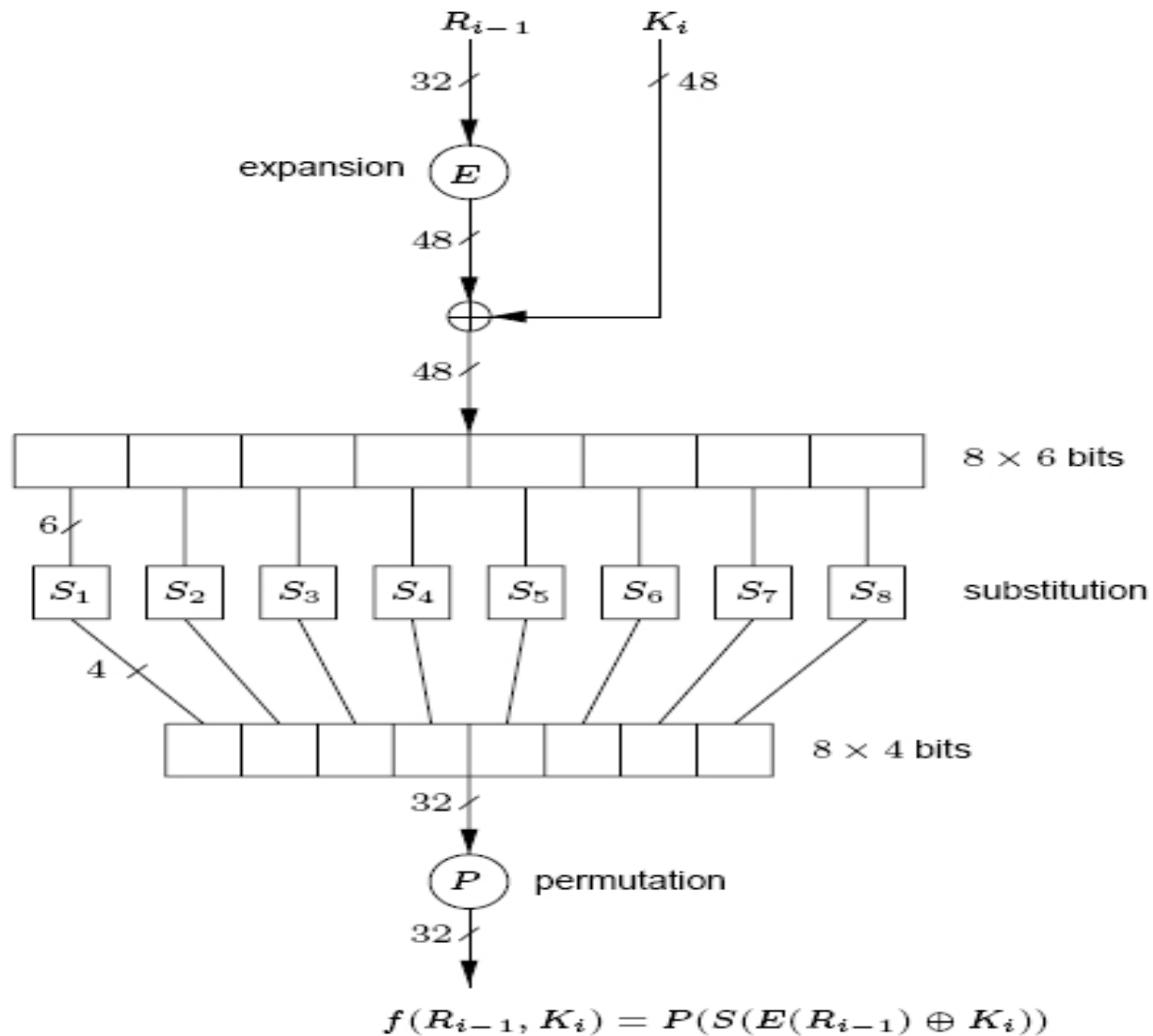
- DES Round Function F can be written as

$$F(R_{i-1}, K_i) = \text{P-Box}(\text{S-Boxes}(\text{Expand}(R_{i-1}) \oplus K_i))$$

F Function



F Function



Expansion

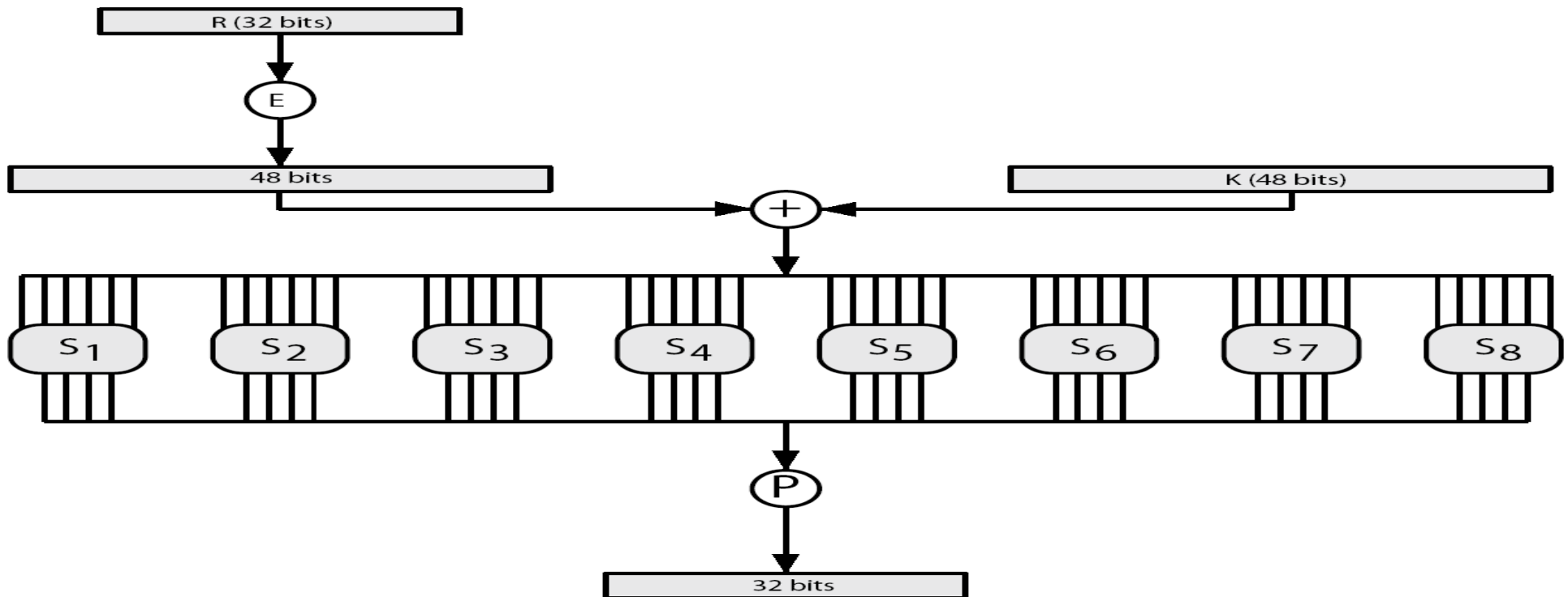
- 32-bit half-block is expanded to 48 bits using the expansion permutation (E) by duplicating half of the bits
- The output consists of 8 6-bit pieces, each containing a copy of 4 corresponding input bits, plus a copy of the immediately adjacent bit from each of the input pieces to either side

Expansion Permutation of E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Key Mixing

- The result is combined with a subkey using an XOR operation.
- Sixteen 48-bit subkeys — one for each round — are derived from the main key using the key schedule



Substitution

- After mixing in the subkey, the block is divided into eight 6-bit pieces before processing by the S-boxes, or substitution boxes.
- Each of the eight S-boxes replaces its six input bits with four output bits according to a non-linear transformation, provided in the form of a lookup table.
- The S-boxes provide the core of the security of DES — without them, the cipher would be linear, and trivially breakable.

S1

S ₁																
	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0yyyy1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
1yyyy0	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
1yyyy1	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S ₂																
	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
0yyyy1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
1yyyy0	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
1yyyy1	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S ₃																
	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
0yyyy1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
1yyyy0	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1yyyy1	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

For example, $S_1(\textcolor{red}{1}0\textcolor{blue}{1}0\textcolor{red}{1}0) = 6 = 0110$.

Final Permutation

- Finally, the 32 outputs from the S-boxes are rearranged according to a fixed permutation, the P-box. This is designed so that, after expansion, each S-box's output bits are spread across 6 different S boxes in the next round.

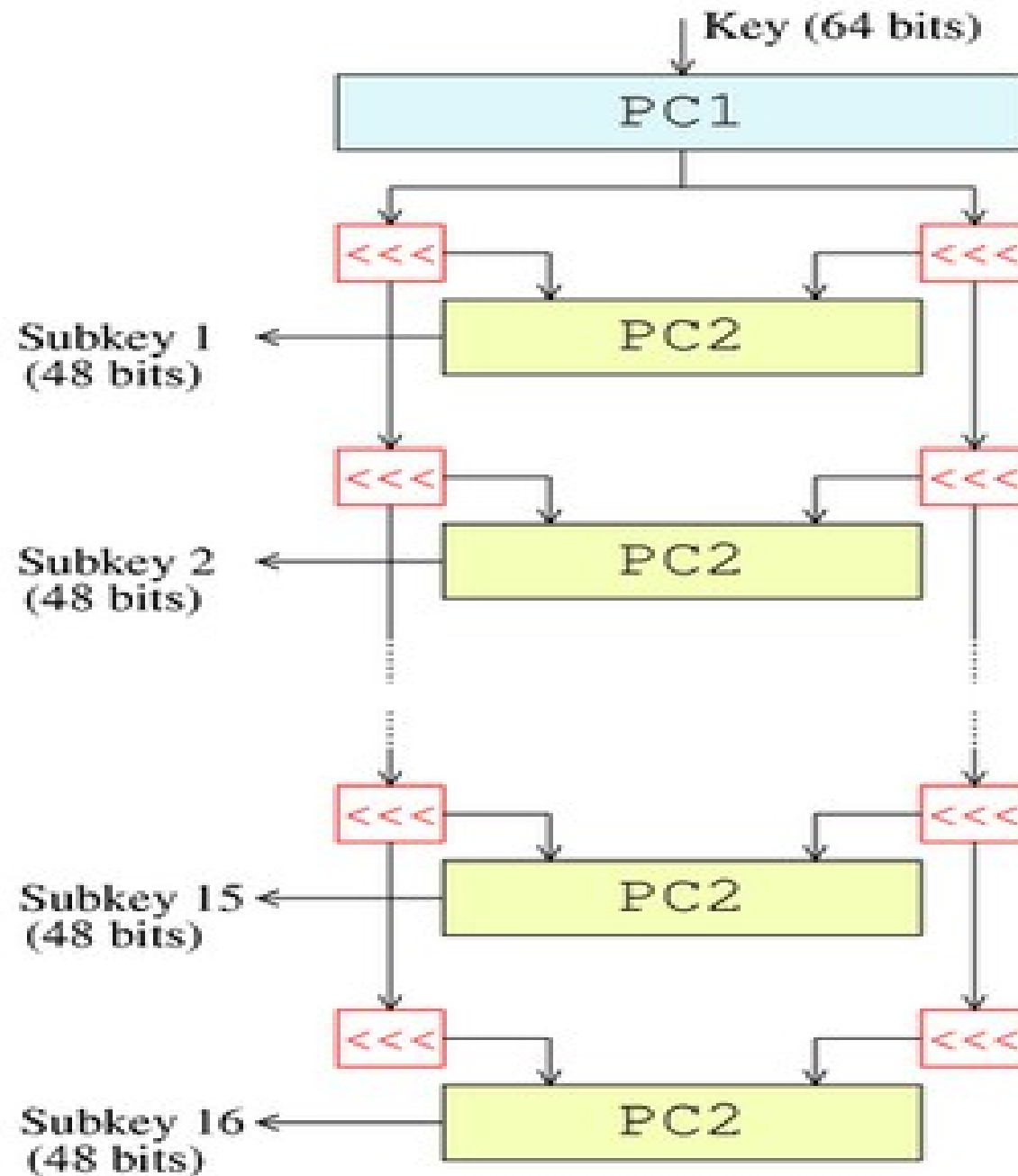
16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Key Schedule

- Initially, 56 bits of the key are selected from the initial 64 by Permuted Choice 1 (PC-1) - the remaining eight bits are either discarded or used as parity check bits
- The 56 bits are then divided into two 28-bit halves; each half is thereafter treated separately
- In successive rounds, both halves are rotated left by one or two bits (specified for each round), and then 48 subkey bits are selected by Permuted Choice 2 (PC-2) — 24 bits from the left half, and 24 from the right

Input Key

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64



Permuted Choice One (PC1)

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Permuted Choice Two (PC2)

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Rotation Number for Each Round

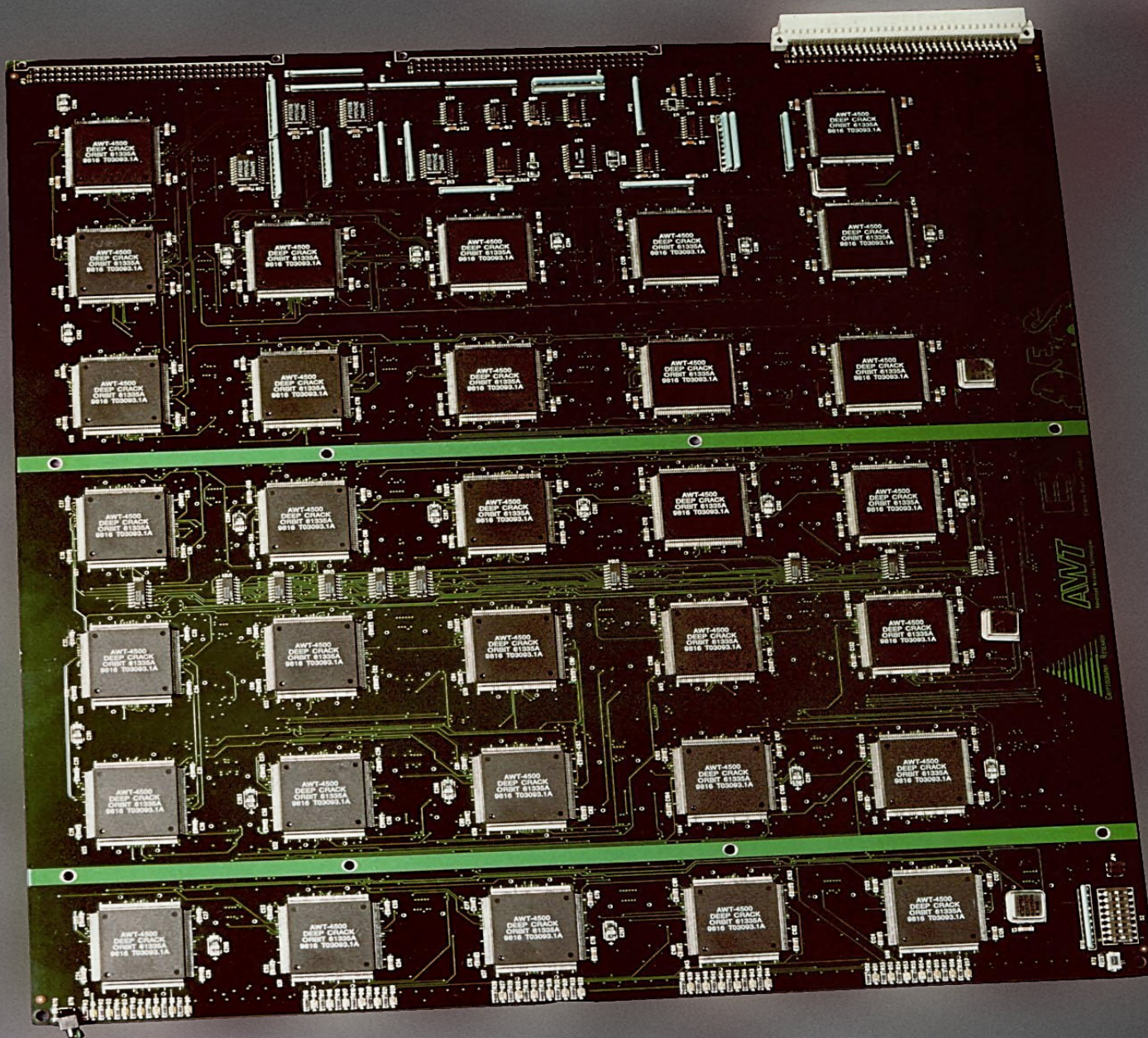
Rotations

Round number	Number of left rotations
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

DES Cracker

- DES Cracker:

- A DES key search machine by Electronic Frontier Foundation (EFF)
- contains 1856 chips
- Cost: \$250,000.
- could search 88 billion keys per second
- won RSA Laboratory's "**DES Challenge II-2**" by successfully finding a DES key in 56 hours.



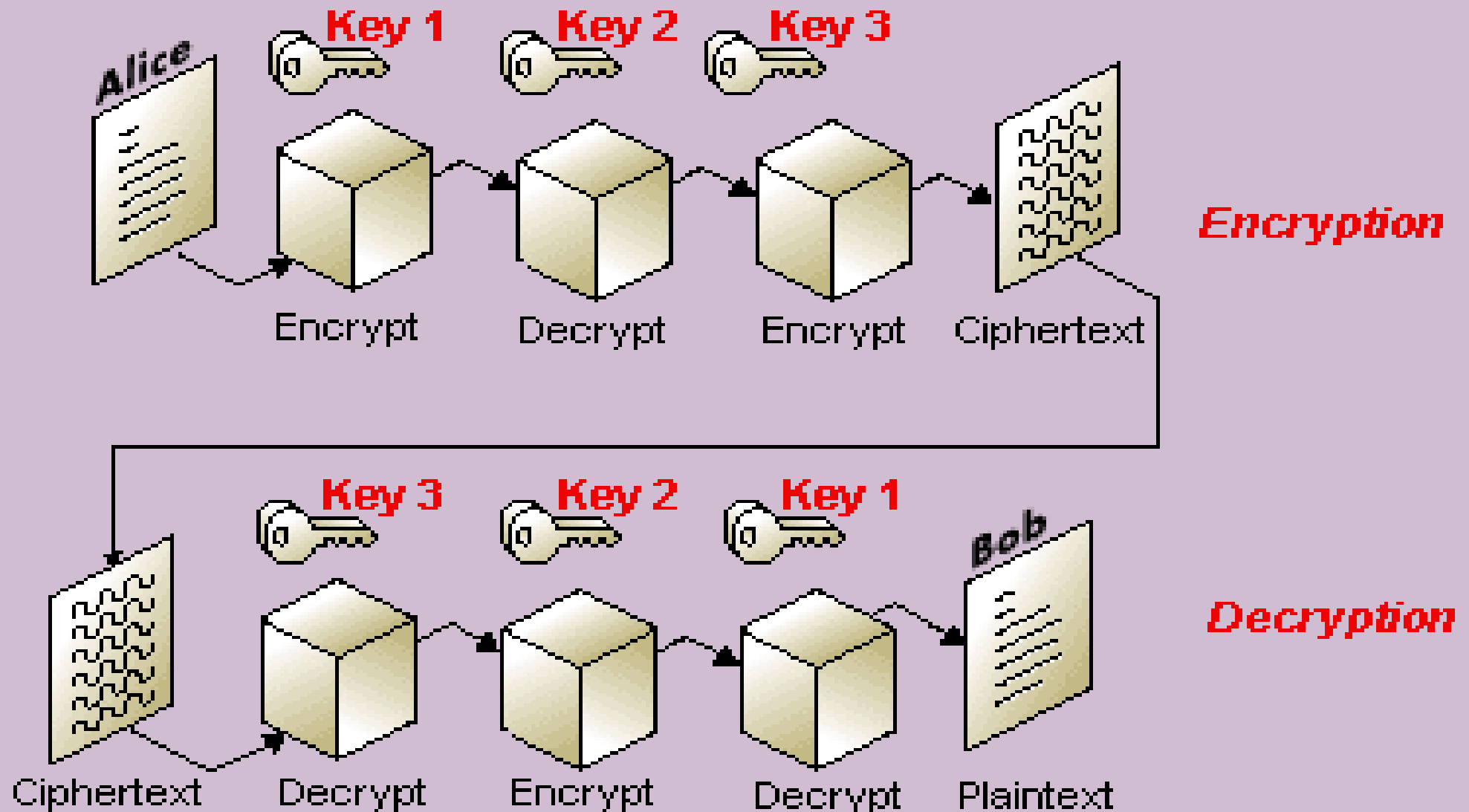
TripleDES

- In 2001, NIST published the Advanced Encryption Standard (AES) to replace DES.
- But users in commerce and finance are not ready to give up on DES.
- As a temporary solution to DES's security problem, one may encrypt a message (with DES) multiple times using multiple keys:
 - 2DES is not much securer than the regular DES
 - So, 3DES with either 2 or 3 keys is used
 - Backward compatible: $E(D(E(P,K),K),K) = E(P,K)$

$$C = E(D(E(P,K1),K2),K1)$$

$$P = D(E(D(C,K1),K2),K1)$$

Symmetric Key (Triple DES) Encryption



AES

- Iterated Block Cipher
- Not a Feistel Cipher
- Block Size: 128 bits
- Key Length: 128, 192, and 256 bits
- Number of rounds : 10, 12, and 14
- Each round uses 4 functions (3 “layers”)
 - ◆ ByteSub (nonlinear layer)
 - ◆ ShiftRow (linear mixing layer)
 - ◆ MixColumn (nonlinear layer)
 - ◆ AddRoundKey (key addition layer)

AES Byte Sub

- Treat 128 bit block as 4x4 byte array
- ByteSub is AES' S-Box

$$\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix} \xrightarrow{\text{ByteSub}} \begin{bmatrix} b_{00} & b_{01} & b_{02} & b_{03} \\ b_{10} & b_{11} & b_{12} & b_{13} \\ b_{20} & b_{21} & b_{22} & b_{23} \\ b_{30} & b_{31} & b_{32} & b_{33} \end{bmatrix}.$$

AES S-Box

Last 4 bits of input

First 4
bits of
input

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

AES Shift Row

- Cyclic Shift Row

$$\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix} \xrightarrow{\text{ShiftRow}} \begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{11} & a_{12} & a_{13} & a_{10} \\ a_{22} & a_{23} & a_{20} & a_{21} \\ a_{33} & a_{30} & a_{31} & a_{32} \end{bmatrix}$$

AES MixColumn

- Invertible, linear operation applied to each column
- Implemented as (big) lookup table

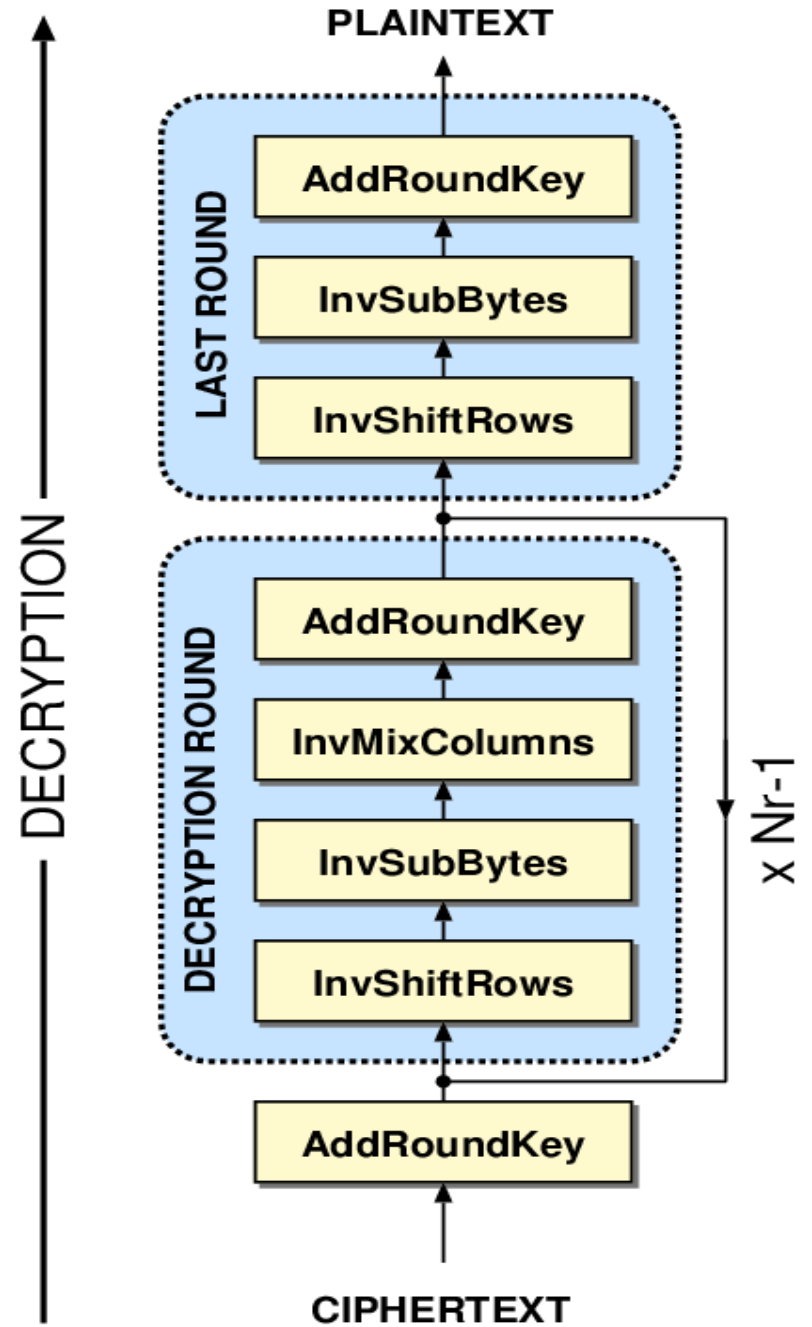
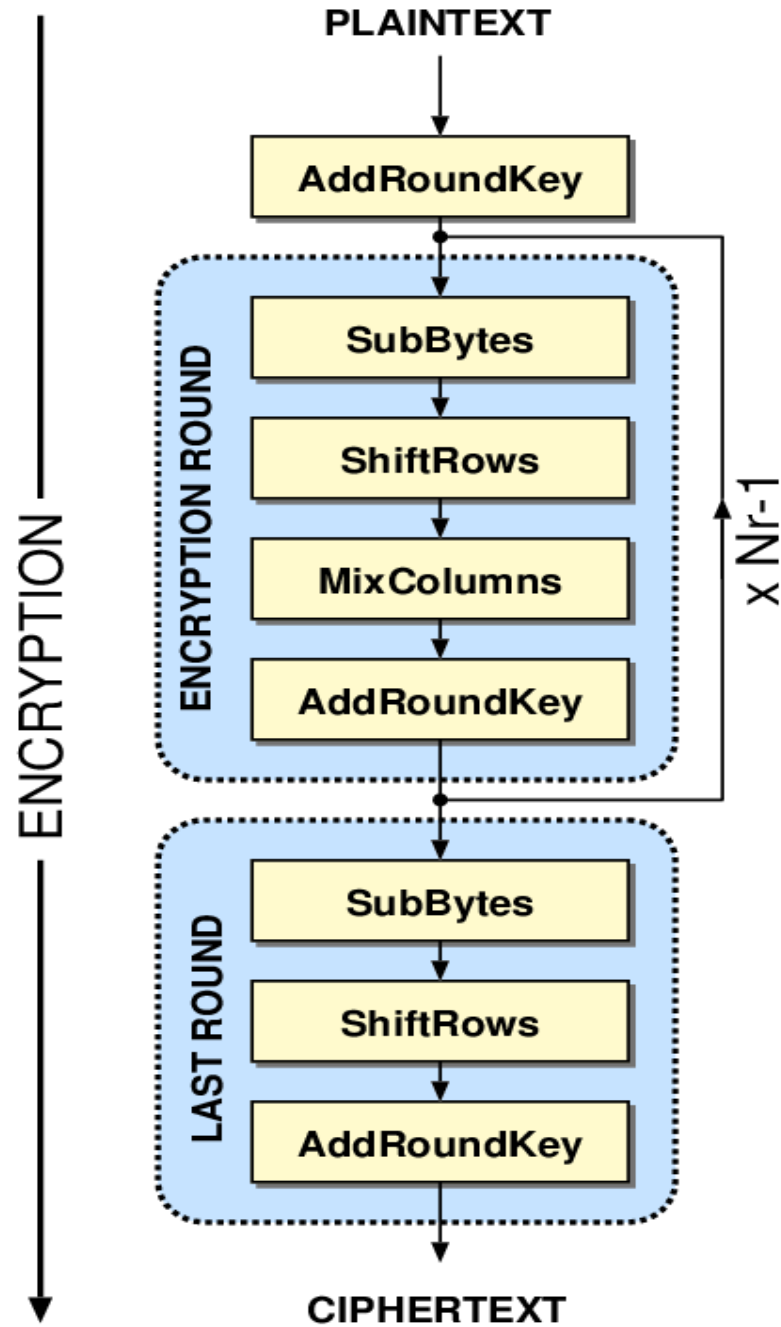
$$\begin{bmatrix} a_{0i} \\ a_{1i} \\ a_{2i} \\ a_{3i} \end{bmatrix} \longrightarrow \text{MixColumn} \longrightarrow \begin{bmatrix} b_{0i} \\ b_{1i} \\ b_{2i} \\ b_{3i} \end{bmatrix} \quad \text{for } i = 0, 1, 2, 3$$

AES AddRoundKey

- XOR subkey with block
- RoundKey (subkey) determined by key schedule algorithm

$$\begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix} \oplus \begin{bmatrix} k_{00} & k_{01} & k_{02} & k_{03} \\ k_{10} & k_{11} & k_{12} & k_{13} \\ k_{20} & k_{21} & k_{22} & k_{23} \\ k_{30} & k_{31} & k_{32} & k_{33} \end{bmatrix} = \begin{bmatrix} b_{00} & b_{01} & b_{02} & b_{03} \\ b_{10} & b_{11} & b_{12} & b_{13} \\ b_{20} & b_{21} & b_{22} & b_{23} \\ b_{30} & b_{31} & b_{32} & b_{33} \end{bmatrix}$$

Block Subkey



Block Ciphers Modes

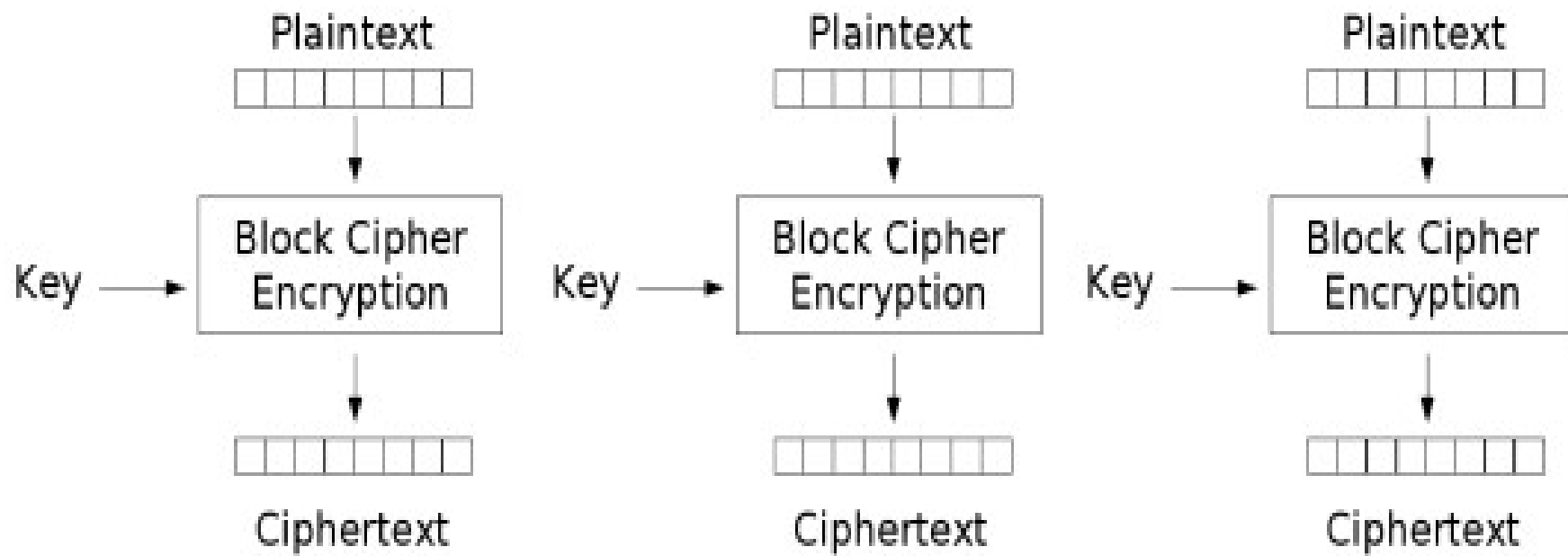
- Stream cipher: length (keystream) = length (plaintext)
- Block cipher: encrypt per block
- Question: how to encrypt multiple blocks?
 - Mode of operation:
 - Partition the message into n-bit blocks
 - Encrypt each separately

Plaintext Blocks : $P_0, P_1, P_2, \dots, P_n$

Encrypt: $C_i = E(P_i, K)$ for $i = 0, 1, 2$

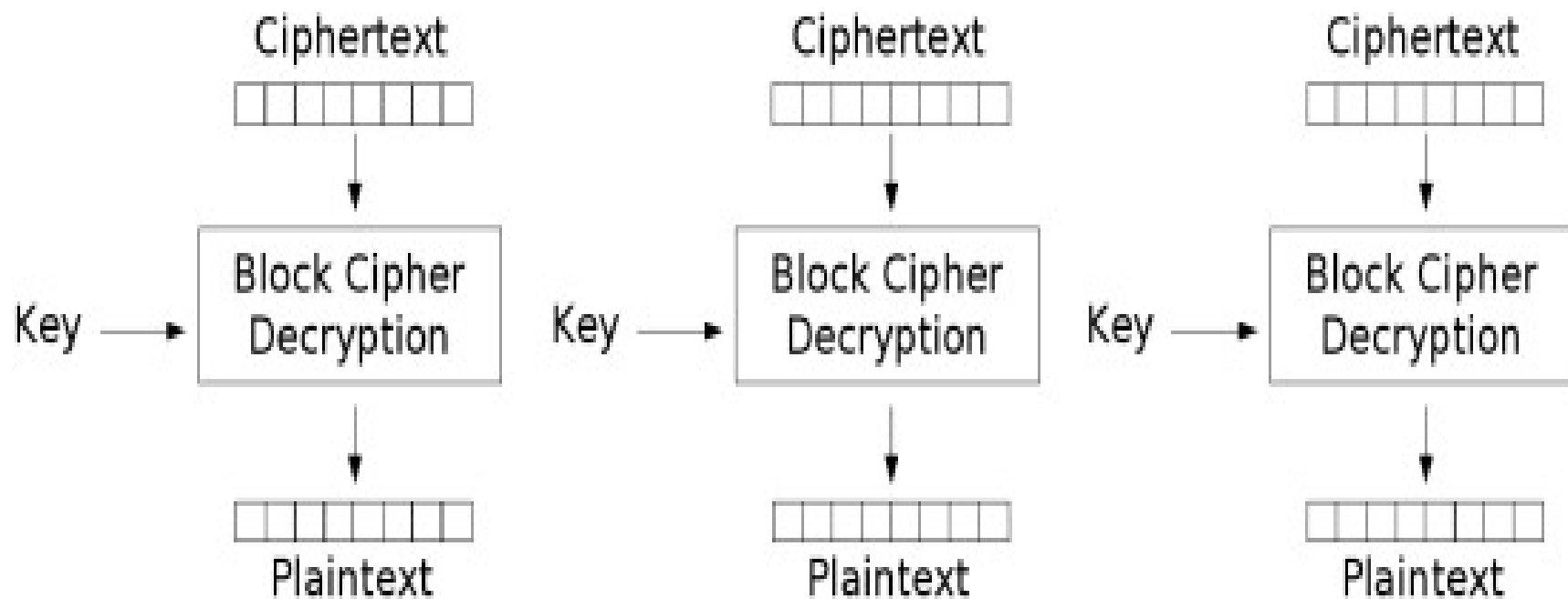
Decrypt: $D(C_i, K)$ for $i = 0, 1, 2$

Electronic codebook (ECB)



Electronic Codebook (ECB) mode encryption

Electronic codebook (ECB)

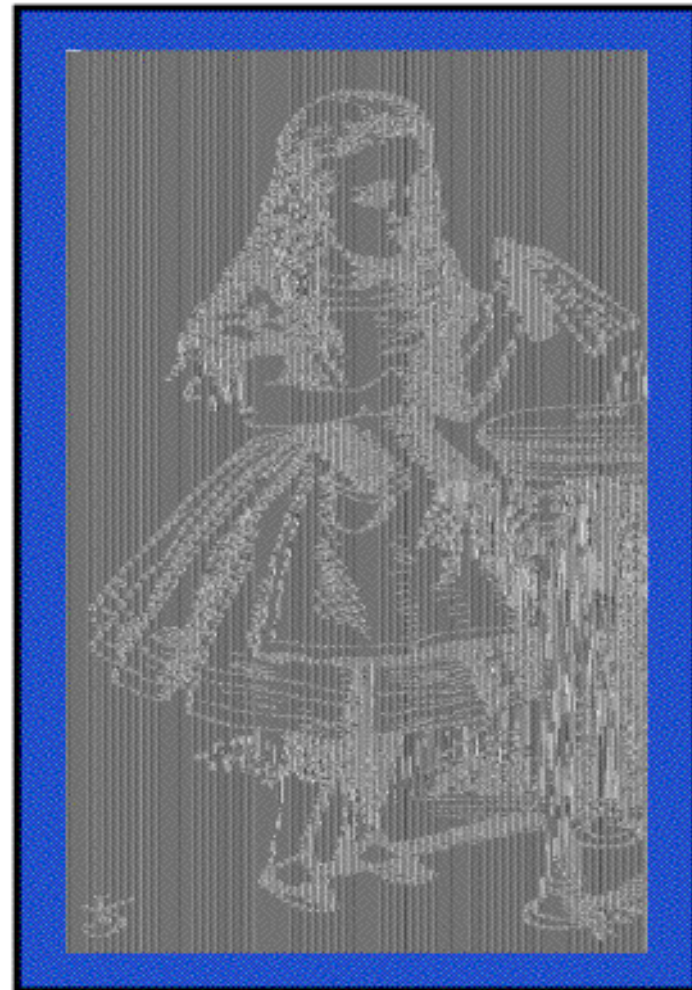


Electronic Codebook (ECB) mode decryption

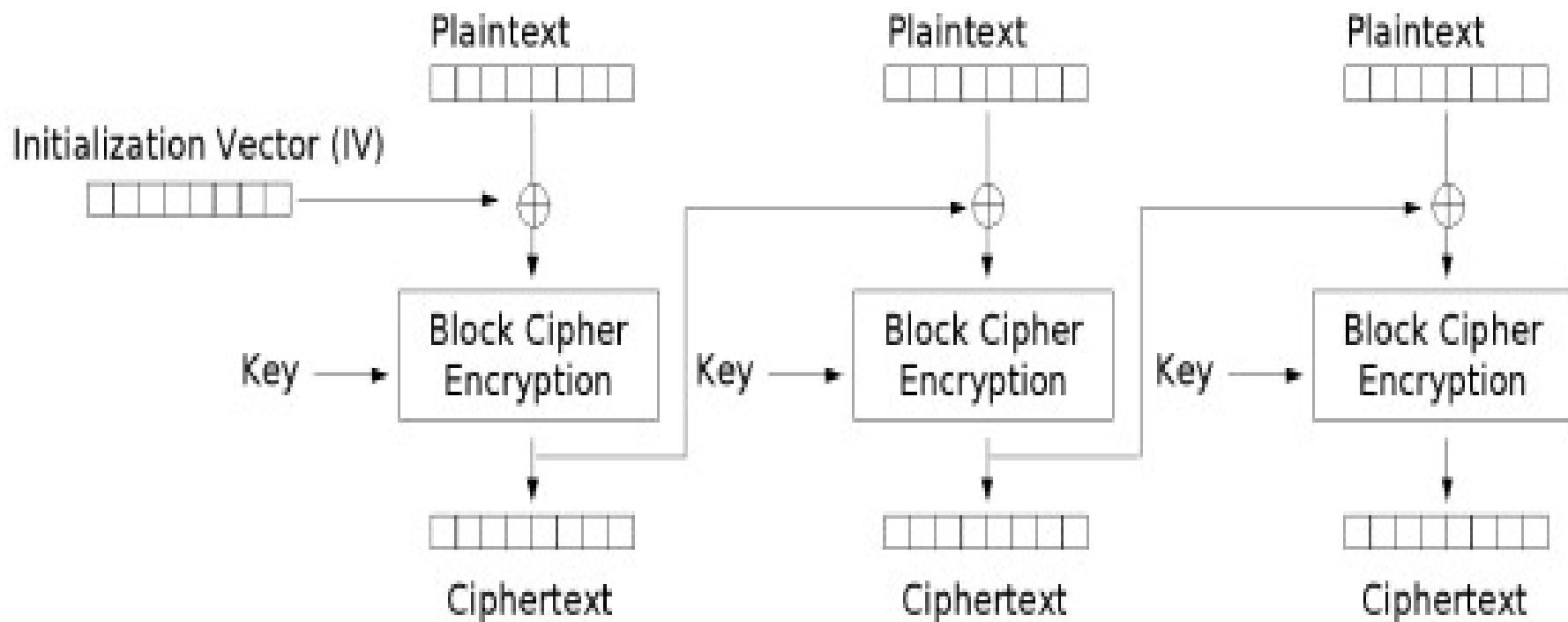
Electronic codebook (ECB)

- Advantages:
 - Simple and easy to design
 - Parallel computing
- Disadvantages:
 - identical plaintext blocks are encrypted into identical ciphertext blocks

Image Encrypted with ECB

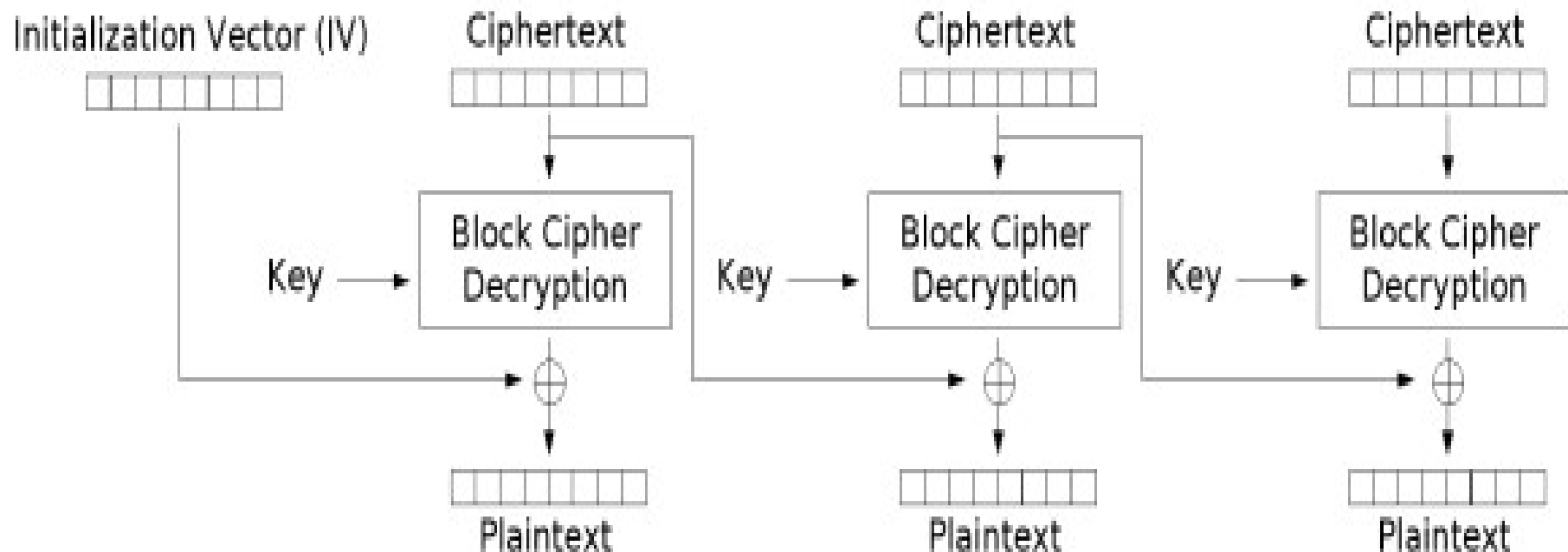


Cipher-block chaining (CBC)



Cipher Block Chaining (CBC) mode encryption

Cipher-block chaining (CBC)

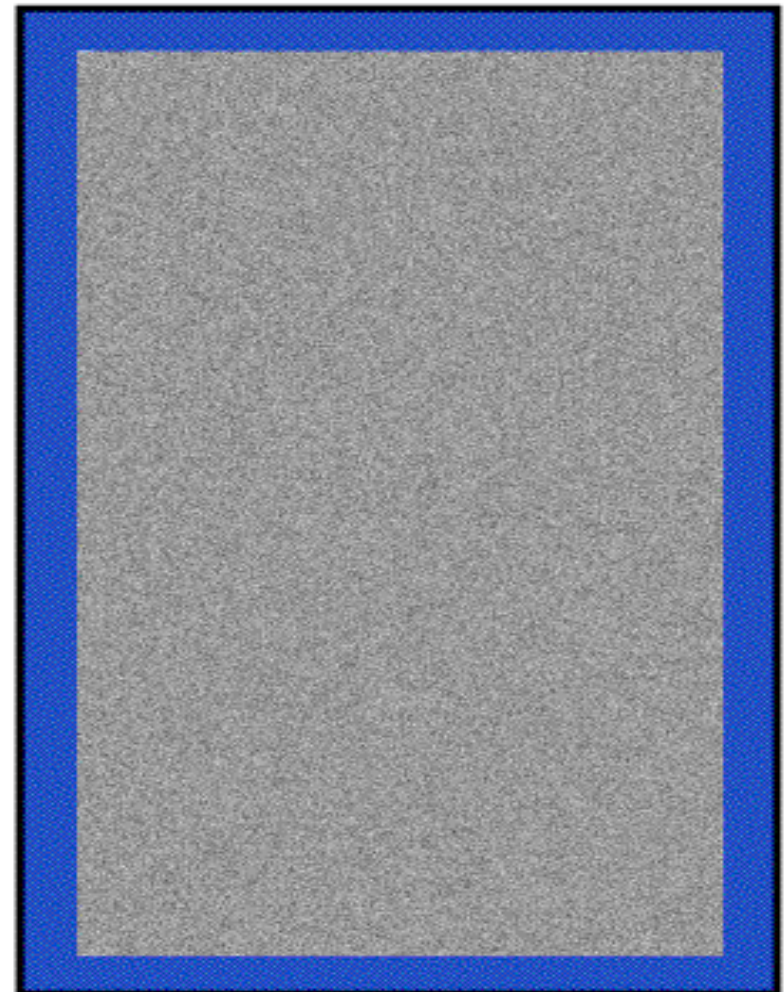


Cipher Block Chaining (CBC) mode decryption

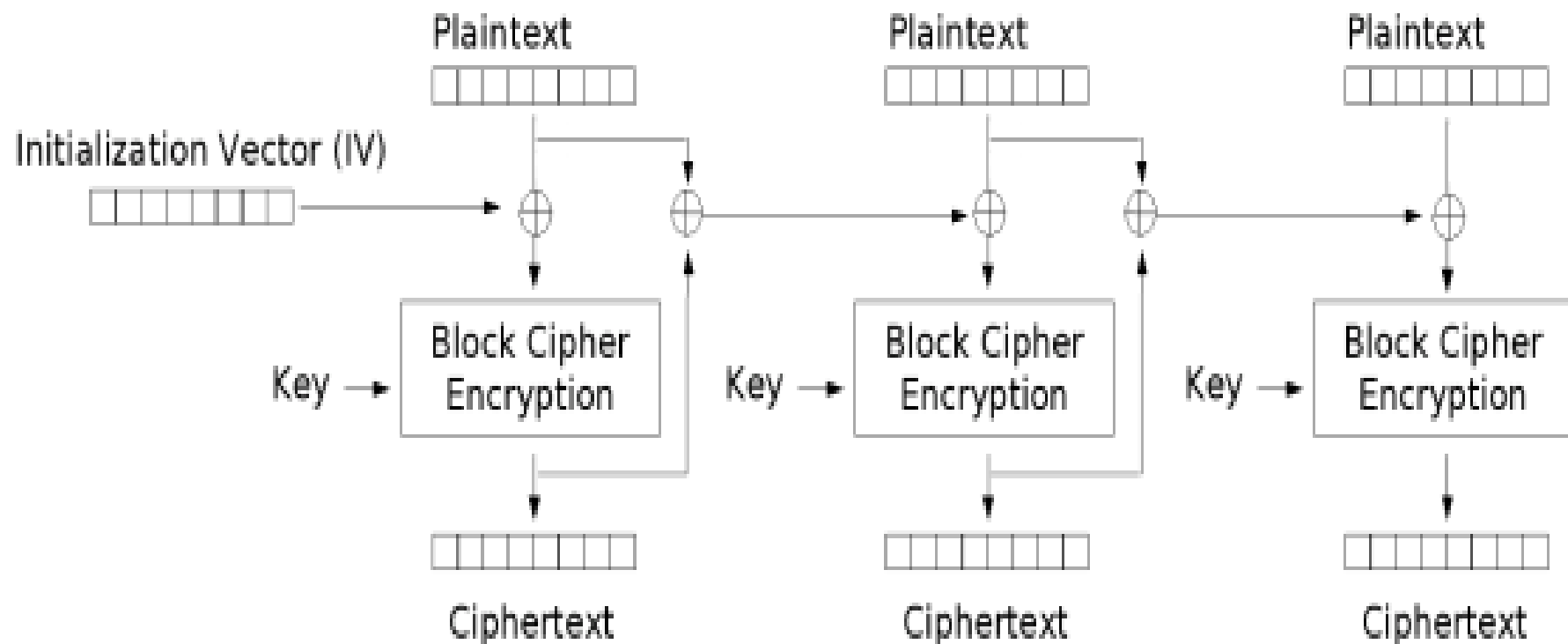
Cipher-block chaining (CBC)

- Advantages:
 - Used in many design
 - A plaintext can be recovered from just two adjacent blocks of ciphertext.
 - As a consequence, decryption can be parallelized,
- Disadvantages:
 - Encryption is sequential → no parallelization
 - Message must be padded to a multiple of the cipher block size

Image Encrypted with CBC

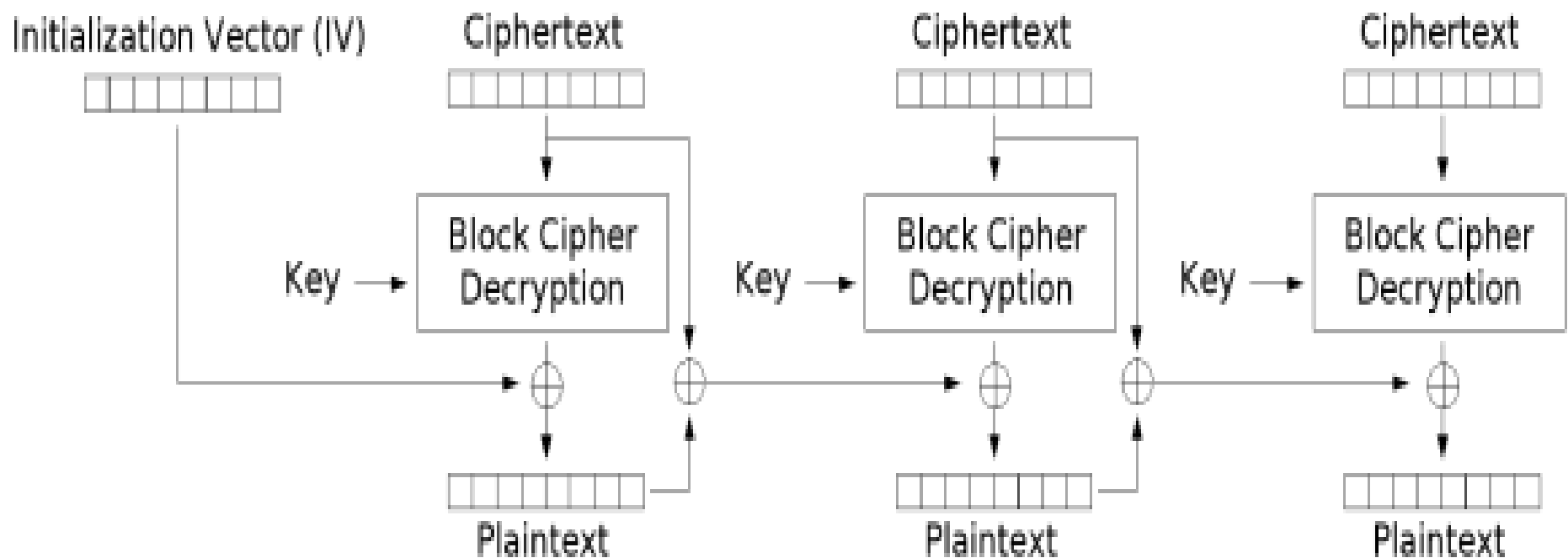


Propagating cipher-block chaining (PCBC)



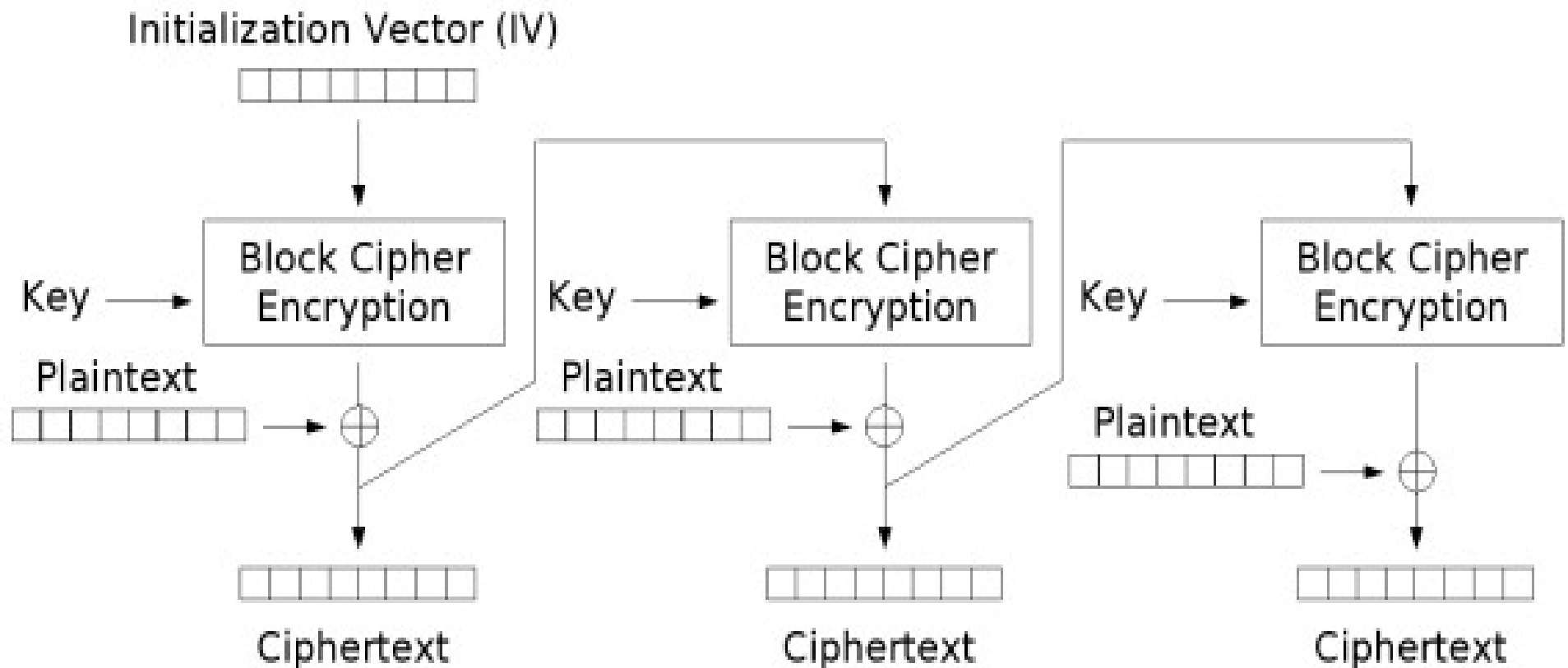
Propagating Cipher Block Chaining (PCBC) mode encryption

Propagating cipher-block chaining (PCBC)



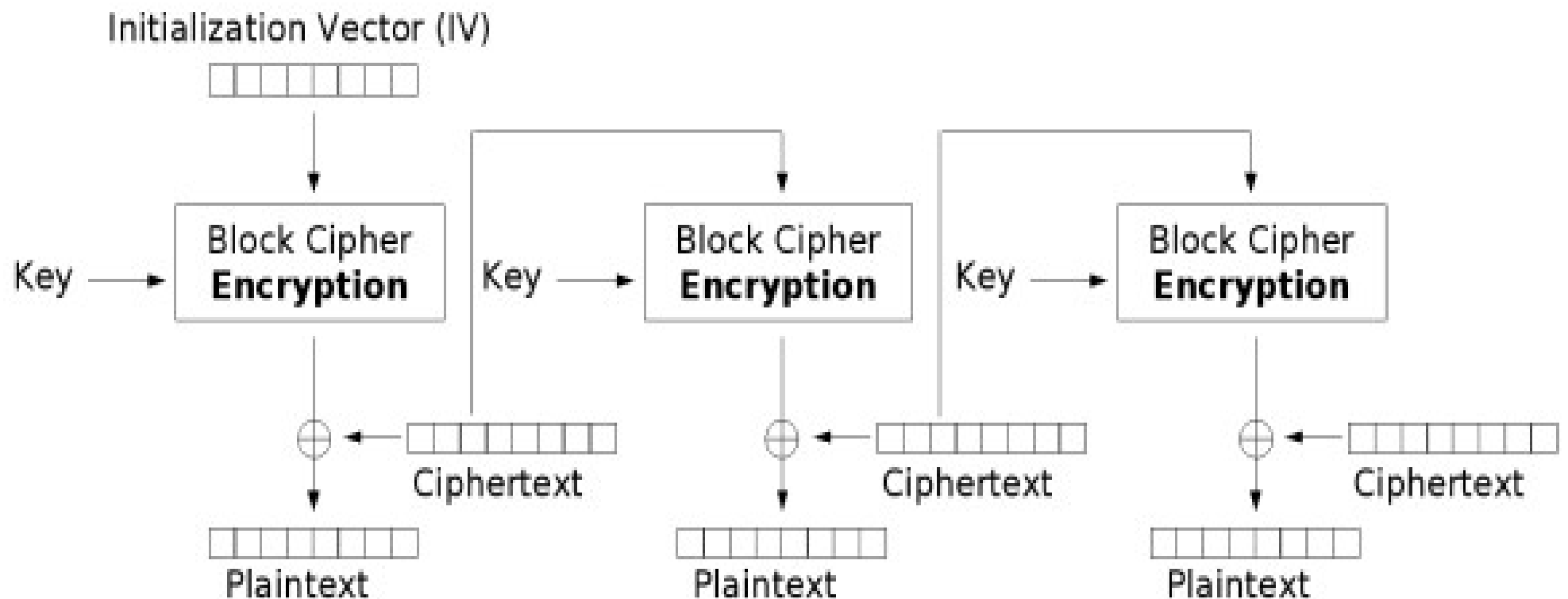
Propagating Cipher Block Chaining (PCBC) mode decryption

Cipher feedback (CFB)



Cipher Feedback (CFB) mode encryption

Cipher feedback (CFB)

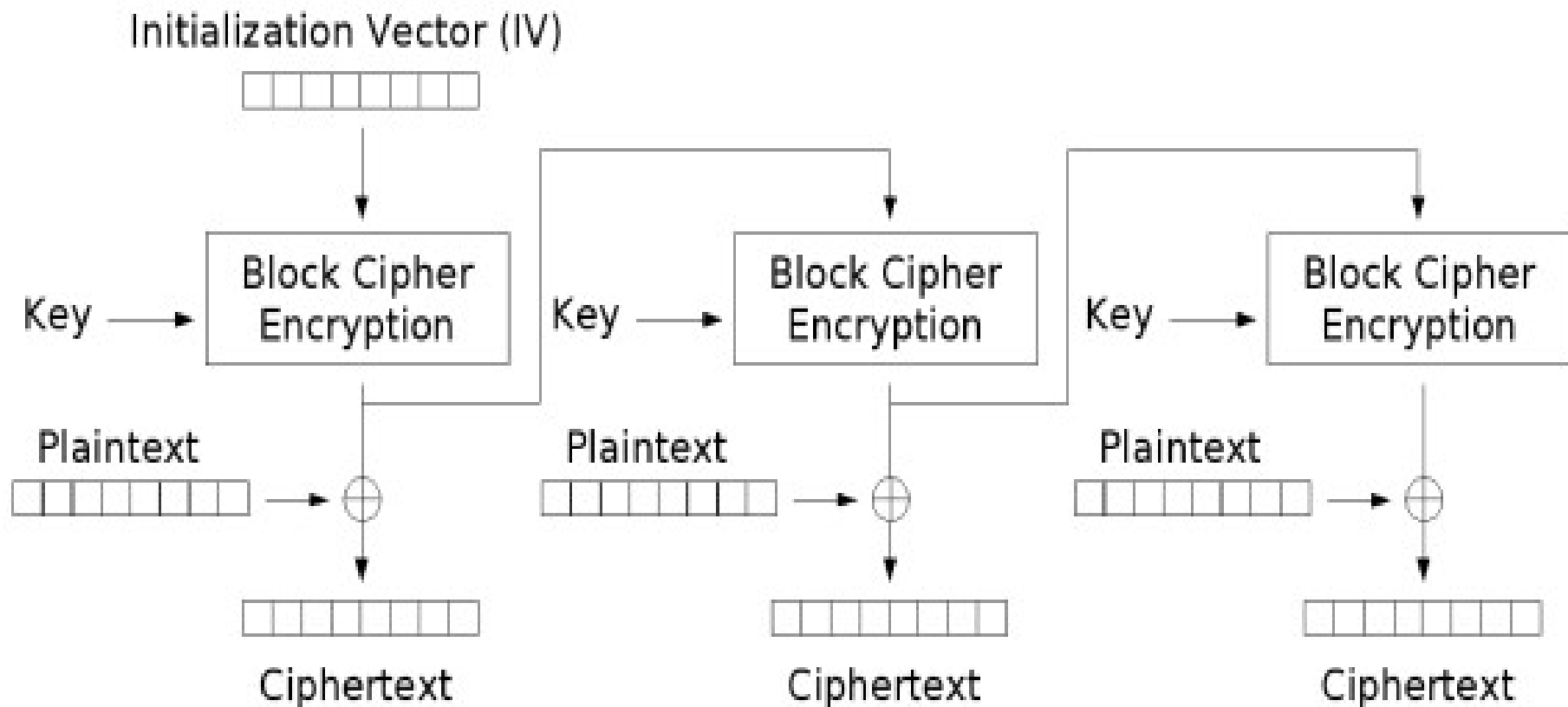


Cipher Feedback (CFB) mode decryption

Cipher feedback (CFB)

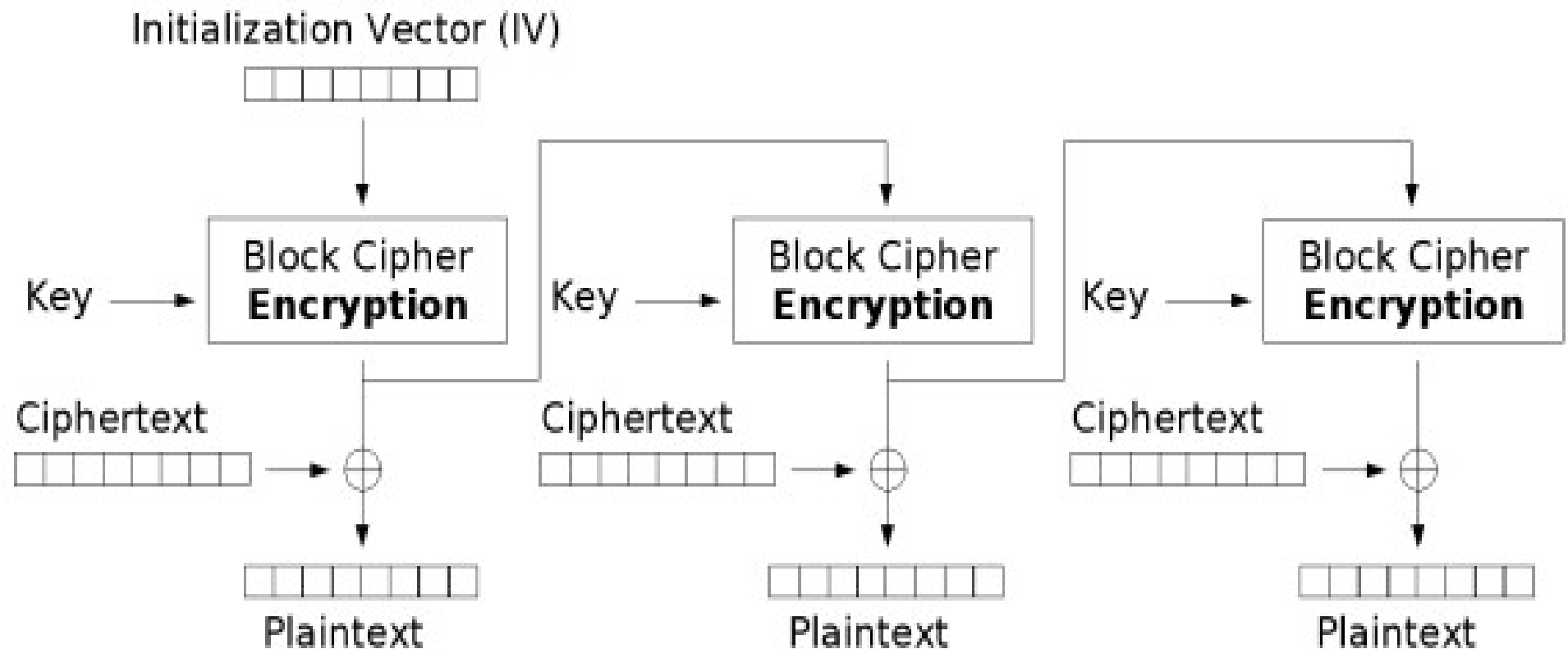
- Advantages
 - Share the same concept as CBC, so decryption can be parallelized
 - Does not require padding
- Disadvantages
 - Changes in the plaintext propagate forever in the ciphertext
 - Encryption cannot be parallelized

Output feedback (OFB)



Output Feedback (OFB) mode encryption

Output feedback (OFB)



Output Feedback (OFB) mode decryption

Padding

- Block cipher works on units of a fixed size
- Messages may come in a variety of lengths
- Final block be padded before encryption
- The simplest is to add null bytes to the plaintext to bring its length up to a multiple of the block size
- C language uses null byte to denote end of string
- CFB and OFB does not require padding
- XORing the plaintext with the output of the block cipher.